ABSTRACT

The invention relates to a method of enciphering/deciphering messages to be exchanged between a secure device (1) and a defined client device (C_j) in a network of client devices as well as to a secure device. The method comprises the steps of:

- performing operations of asymmetric cryptography by the secure device (1) and by the defined client device (C_j) respectively with the aid of a private key (n_j, d_j) and of a public key (n_j, e_j), and

- determining the private key (n_j, d_j) corresponding to the public key (n_j, e_j) of the defined client device (C_j), on the basis of a secret master key (MK) stored in the secure device, and at least one public data item (n_j, CID_j) dispatched by the defined client device (C_j).

Figure 5